Chapter 2 Resource

Incident Response (IR), Business Continuity (BC) and Disaster Recovery (DR)

Chapter Summary

This chapter focused mainly on the availability part of the CIA triad and the importance of maintaining availability for business operations. Maintaining business operations during or after an incident, event, breach, intrusion, exploit or zero day is accomplished through the implementation of Incident Response (IR), Business Continuity (BC), and/or Disaster Recovery (DR) plans. While these three plans may seem to overlap in scope, they are three distinct plans that are vital to the survival of any organization facing out of the ordinary operating conditions. Here are the primary things to remember from this chapter:

First, the Incident Response plan responds to abnormal operating conditions to keep the business operating. The four main components of Incident Response are: Preparation; Detection and Analysis; Containment, Eradication and Recovery; and Post-Incident Activity. Incident Response teams are typically a cross-functional group of individuals who represent the management, technical and functional areas of responsibility most directly impacted by a security incident. The team is trained on incident response and the organization's incident response plan. When an incident occurs, the team is responsible for determining the amount and scope of damage and whether any confidential information was compromised, implementing recovery procedures to restore security and recover from incident-related damage, and supervising implementation of future measures to improve security and prevent recurrence of the incident.

Second, the Business Continuity plan is designed to keep the organization operating through the crisis. Components of the Business Continuity plan include details about how and when to enact the plan and notification systems and call trees for alerting the team members and organizational associates that the plan has been enacted. In addition, it includes contact numbers for contacting critical third-party partners, external emergency providers, vendors and customers. The plan provides the team with immediate response procedures and checklists and guidance for management.

Finally, if both the Incident Response and Business Continuity plans fail, the Disaster Recovery plan is activated to return operations to normal as quickly as possible. The Disaster Recovery plan may include the following components: executive summary providing a high-level overview of the plan, department-specific plans, technical guides for IT personnel responsible for implementing and maintaining critical backup systems, full copies of the plan for critical disaster recovery team members, and checklists for certain individuals.

Module Names

Module 1: Understand Incident Response (IR)

Module 2: Understand Business Continuity (BC)

Module 3: Understand Disaster Recovery (DR)

Chapter to Domain Mapping

Module Number	Module Title	Domains
1	Understand Incident Response (IR)	2.3, 2.3.1, 2.3.2, 2.3.3
2	Understand Business Continuity (BC)	2.1, 2.1.1, 2.1.2, 2.1.3
3	Understand Disaster Recovery (DR)	2.2, 2.2.1, 2.2.2, 2.2.3

Learning Objectives

After completing this chapter, the participant will be able to:

- Explain how organizations respond to, recover from and continue to operate during unplanned disruptions
- Recall the terms and components of incident response
- Summarize the components of a business continuity plan
- Identify the components of disaster recovery
- Practice the terminology of and review business continuity, disaster recovery and incident response concepts

Chapter Takeaways

Module 1: Understand Incident Response (IR)

Incident Response Terminology:

- Breach
- Event
- Exploit
- Incident
- Intrusion
- Threat
- Vulnerability
- Zero Day

Four main components of Incident Response are:

- Preparation
- Detection and Analysis
- Containment, Eradication and Recovery
- Post-Incident Activity

Three possible models for an Incident Response Team (IRT):

- Leveraged
- Dedicated
- Hybrid

Module 2: Understand Business Continuity (BC)

Components of a Business Continuity (BC) plan include:

- List of the BCP team members, including multiple contact methods and backup members
- Immediate response procedures and checklists (security and safety procedures, fire suppression procedures, notification of appropriate emergency-response agencies, etc.)
- Notification systems and call trees for alerting personnel that the BCP is being enacted
- Guidance for management, including designation of authority for specific managers
- How/when to enact the plan
- Contact numbers for critical members of the supply chain (vendors, customers, possible external emergency providers, third-party partners)

Chapter Takeaways (Continued)

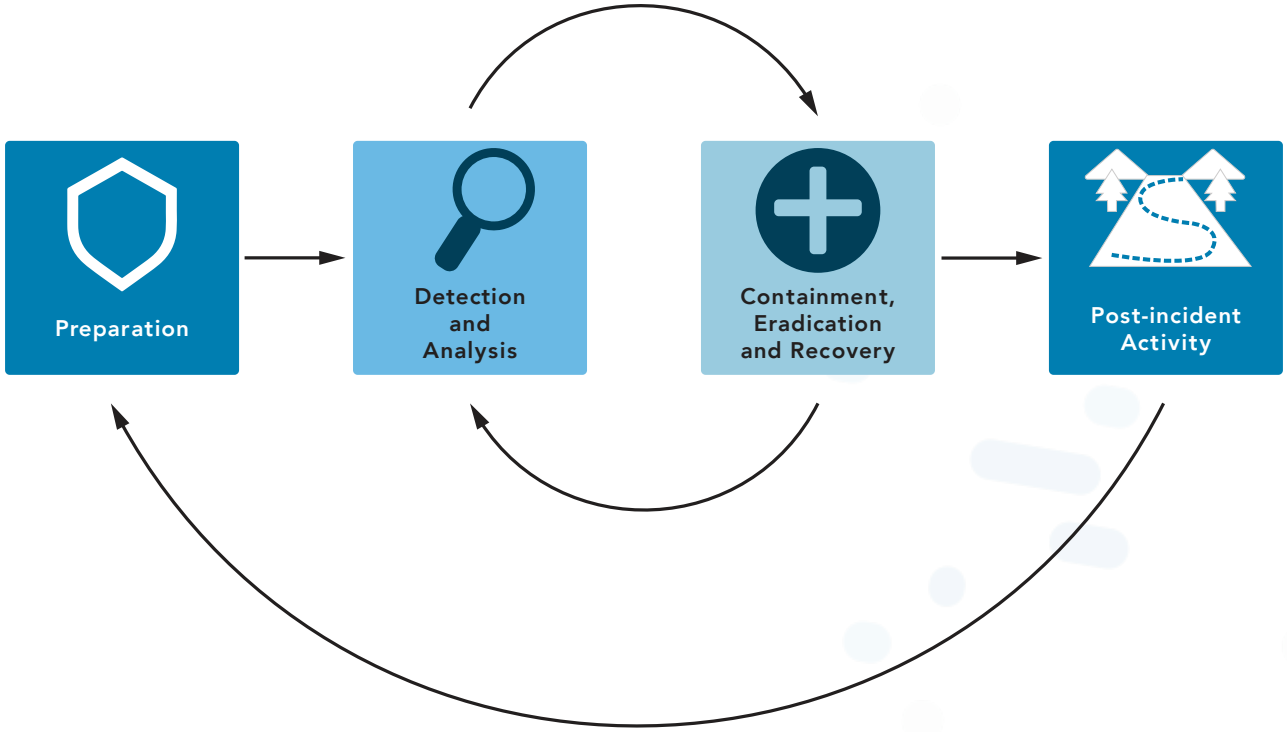
Module 3: Understand Disaster Recovery (DR)

Five possible components to include in a Disaster Recovery (DR) plan:

1. Executive summary providing a high-level overview of the plan
2. Department-specific plans
3. Technical guides for IT personnel responsible for implementing and maintaining critical backup systems
4. Full copies of the plan for critical disaster recovery team members
5. Checklists for certain individuals

Graphics

Components of an Incident Response Plan



Knowing the components of and their relationship to each other will help you build and follow an Incident Response Plan.

Chapter Terms and Definitions

Adverse Events

Events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, defacement of a web page or execution of malicious code that destroys data.

Breach

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for other than an authorized purpose. Source: NIST SP 800-53 Rev. 5

Business Continuity (BC)

Actions, processes and tools for ensuring an organization can continue critical operations during a contingency.

Business Continuity Plan (BCP)

The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

Business Impact Analysis (BIA)

An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. NIST SP 800-34 Rev. 1

Disaster Recovery (DR)

In information systems terms, the activities necessary to restore IT and communications services to an organization during and after an outage, disruption or disturbance of any kind or scale.

Disaster Recovery Plan (DRP)

The processes, policies and procedures related to preparing for recovery or continuation of an organization's critical business functions, technology infrastructure, systems and applications after the organization experiences a disaster. A disaster is when an organization's critical business function(s) cannot be performed at an acceptable level within a predetermined period following a disruption.

Event

Any observable occurrence in a network or system. Source: NIST SP 800-61 Rev 2

Exploit

A particular attack. It is named this way because these attacks exploit system vulnerabilities.

Incident

An event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits.

Incident Handling

The mitigation of violations of security policies and recommended practices. Source: NIST SP 800-61 Rev 2

Incident Response (IR)

The mitigation of violations of security policies and recommended practices. Source: NIST SP 800-61 Rev 2

Incident Response Plan (IRP)

The documentation of a predetermined set of instructions or procedures to detect, respond to and limit consequences of a malicious cyberattack against an organization's information systems(s). Source: NIST SP 800-34 Rev 1

Intrusion

A security event, or combination of security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization. Source: IETF RFC 4949 Ver 2

Security Operations Center

A centralized organizational function fulfilled by an information security team that monitors, detects and analyzes events on the network or system to prevent and resolve issues before they result in business disruptions.

Vulnerability

Weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source. Source: NIST SP 800-128.

Zero Day

A previously unknown system vulnerability with the potential of exploitation without risk of detection or prevention because it does not, in general, fit recognized patterns, signatures or methods.